Message Variance Convergence Condition for Generalizations of LDLC lattices

Brian M. Kurkoski Japan Advanced Institute of Science and Technology

Information Theory Workshop
Hobart, Tasmania, Australia
2 November 2014

Semi-Tutorial on Low-Density Lattice Codes

Brian M. Kurkoski Japan Advanced Institute of Science and Technology

Information Theory Workshop
Hobart, Tasmania, Australia
2 November 2014

Low-Density Lattice Codes

LDLC lattices were described by Sommer, Shalvi and Feder [IT 2008]

- Inverse generator matrix $H = G^{-1}$ is sparse
- Decoding using Gaussian belief-propagation
- high dimension, $n = 100, 1000, 10000, 100000$

Low-Density Lattice Codes

LDLC lattices were described by Sommer, Shalvi and Feder [IT 2008]

- Inverse generator matrix $H = G^{-1}$ is sparse
- Decoding using Gaussian belief-propagation
- high dimension, $n = 100, 1000, 10000, 100000$
- come within 0.6 dB of unconstrained capacity
- spatially-coupled LDLCs come with 0.35 dB of unconstrained capacity

Merits of LDLC constructions

- High-dimension lattice design in the Euclidean space
- Fits naturally with many aspects of lattice theory
- Gaussian BP decoding is interesting

Tour of LDLC Lattices

1. Basics of LDLCs:

    1a LDLC Latin Square construction

    1b Encoding

    1c Decoding

    1d Design

2. Convergence condition with a new perspective
3. Gaussian belief-propagation decoding
4. LDLC vs. LDPC-based Construction A lattices
5. Open problems

Definitions

n is lattice dimension

$\mathbf{x}$ is lattice point

$\mathbf{b}$ is integer vector

G is generator matrix

$$\mathbf{x} = G\,\mathbf{b}$$

inverse generator matrix $H = \mathrm{G}^{-1}$

$$H\,\mathbf{x} = \mathbf{b}$$

(1a) LDLC "Latin Square" Construction

H has constant row and column weight d.

Latin square: each row/column $\{h_1, h_2, \ldots, h_d\}$ with random $\pm$, $h_1 \geq h_2 \geq \ldots \geq h_d$

Necessary condition:

$$\alpha = \frac{\sum_{i=2}^{d} h_i^2}{h_1^2} \leq 1$$

- Choose $h_1 = 1$

  (forces $|\det H|$ to be $= 1$)
- Non-zero elts pseudo-random loc.
- Random sign changes

$$\begin{bmatrix} 1/2 & 0 & 0 & 0 & 1 & 0 & 0 & -1/3 \\ 0 & -1 & 0 & 0 & 0 & 1/3 & 1/2 & 0 \\ 0 & 0 & -1 & 1/3 & 0 & -1/2 & 0 & 0 \\ 1/3 & 0 & -1/2 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1/2 & 1/3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/3 & 1 & 0 & -1/2 \\ -1 & 0 & 0 & 0 & 1/2 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & -1/2 & 0 & 0 & 0 & -1 \end{bmatrix}$$

LDLC "Latin Square" Construction

Example: row/column weight 3

elements from $\{1, 1/2, 1/3\}$

$$H = \begin{bmatrix} 1/2 & 0 & 0 & 0 & 1 & 0 & 0 & -1/3 \\ 0 & -1 & 0 & 0 & 0 & 1/3 & 1/2 & 0 \\ 0 & 0 & -1 & 1/3 & 0 & -1/2 & 0 & 0 \\ 1/3 & 0 & -1/2 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1/2 & 1/3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/3 & 1 & 0 & -1/2 \\ -1 & 0 & 0 & 0 & 1/2 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & -1/2 & 0 & 0 & 0 & -1 \end{bmatrix}$$

LDLC "Latin Square" Construction

Example: row/column weight 3

elements from {1, 1/2, 1/3}

$$H = \begin{bmatrix} 1/2 & 0 & 0 & 0 & 1 & 0 & 0 & -1/3 \\ 0 & -1 & 0 & 0 & 0 & 1/3 & 1/2 & 0 \\ 0 & 0 & -1 & 1/3 & 0 & -1/2 & 0 & 0 \\ 1/3 & 0 & -1/2 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1/2 & 1/3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/3 & 1 & 0 & -1/2 \\ -1 & 0 & 0 & 0 & 1/2 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & -1/2 & 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\alpha = \frac{(\frac{1}{2})^2 + (\frac{1}{3})^2}{1^2} = \frac{11}{36} \leq 1$$

(1b) Encoding LDLC codes

$$\mathbf{x} = G\mathbf{b} \longleftarrow \text{don't want to compute } H^{-1}$$

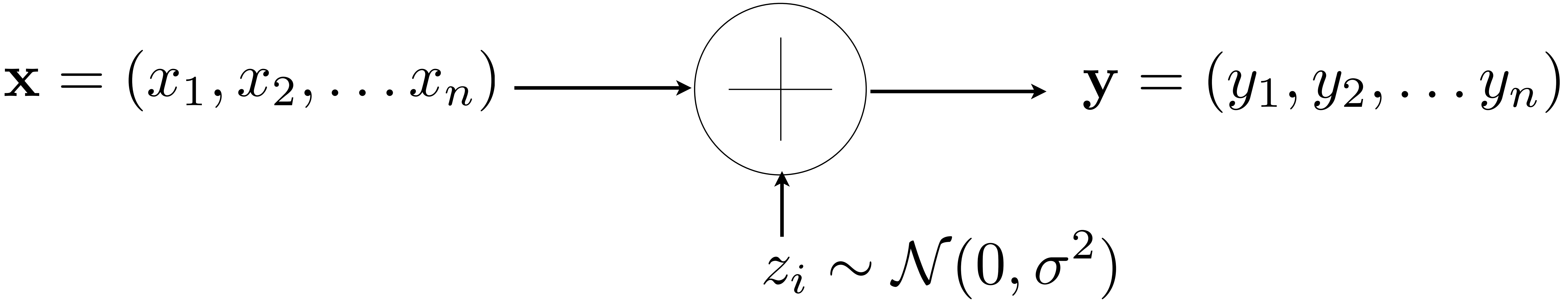
$$H\mathbf{x} = \mathbf{b} \longleftarrow \text{system of equations unknown } \mathbf{x}$$

Encoding using Jacobi method or Gauss-Seidel method.

Encoding can be performed without G.

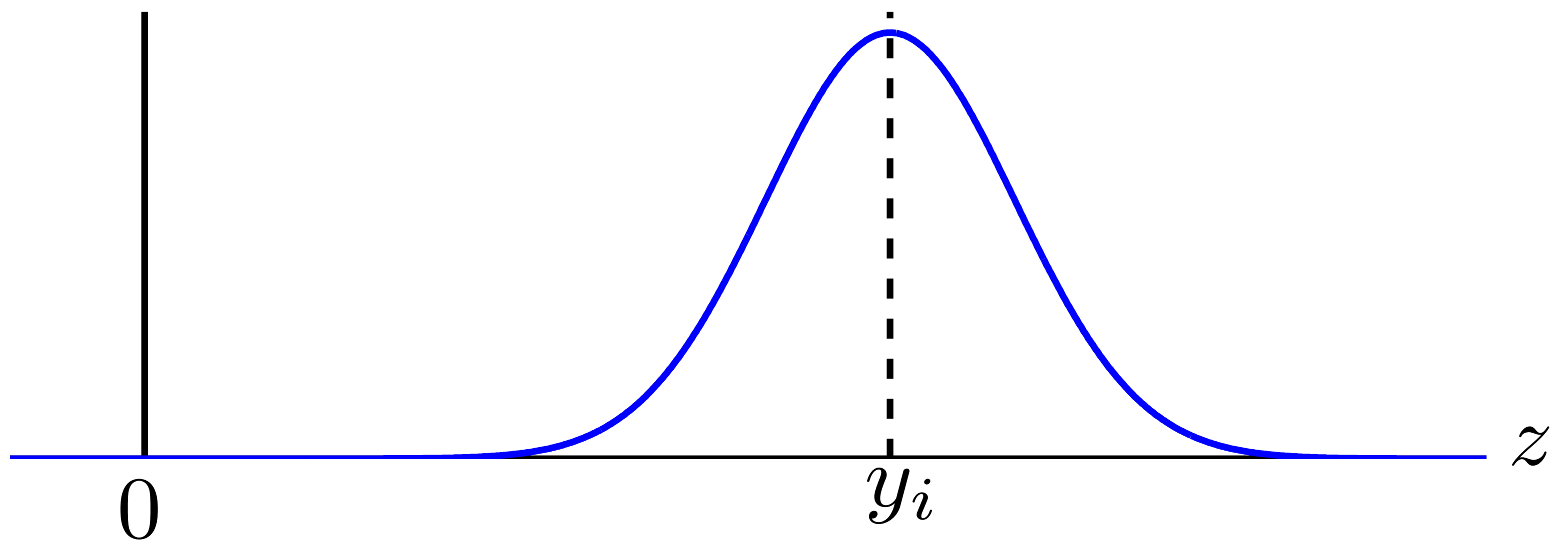
Channel and Initial Message

A lattice point $\mathbf{x}$ is transmitted over an AWGN channel

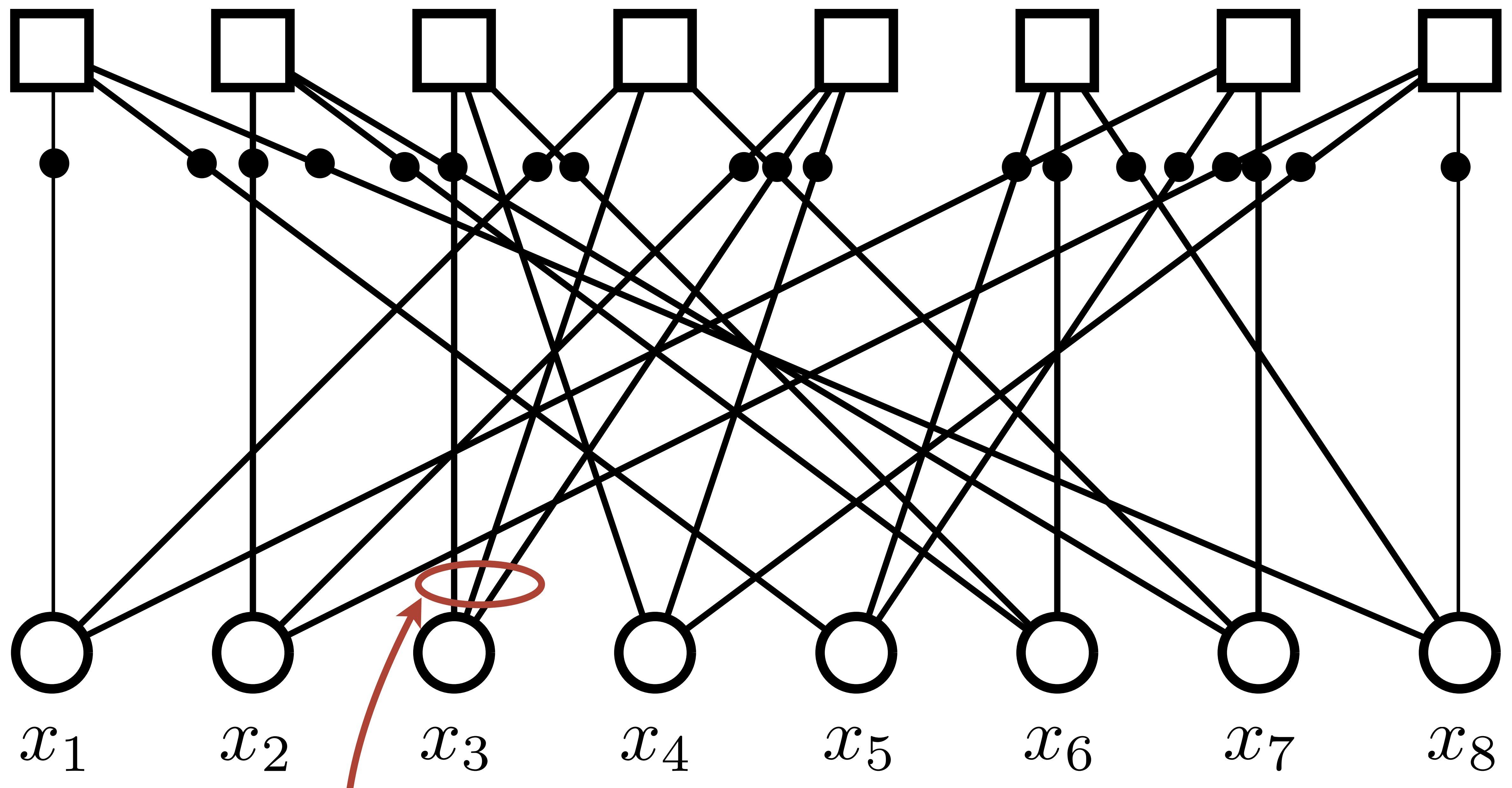


Channel message $Y_i(z)$ is Gaussian mean y_i, variance σ^2:

$$Y_i(z) \quad = \quad \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(z-y_i)^2/2\sigma^2}$$



(1c) Decoding: Tanner Graph



$$\begin{bmatrix} 1/2 & 0 & 0 & 0 & 1 & 0 & 0 & -1/3 \\ 0 & -1 & 0 & 0 & 0 & 1/3 & 1/2 & 0 \\ 0 & 0 & -1 & 1/3 & 0 & -1/2 & 0 & 0 \\ 1/3 & 0 & -1/2 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1/2 & 1/3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/3 & 1 & 0 & -1/2 \\ -1 & 0 & 0 & 0 & 1/2 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & -1/2 & 0 & 0 & 0 & -1 \end{bmatrix}$$

each edge has exactly one:

h_1, h_2, h_3, ... edge

LDLC Iterative Decoding

Variables are real numbers

Messages $R(z)$ is a function

$$R(z) = \Pr(x = z)$$

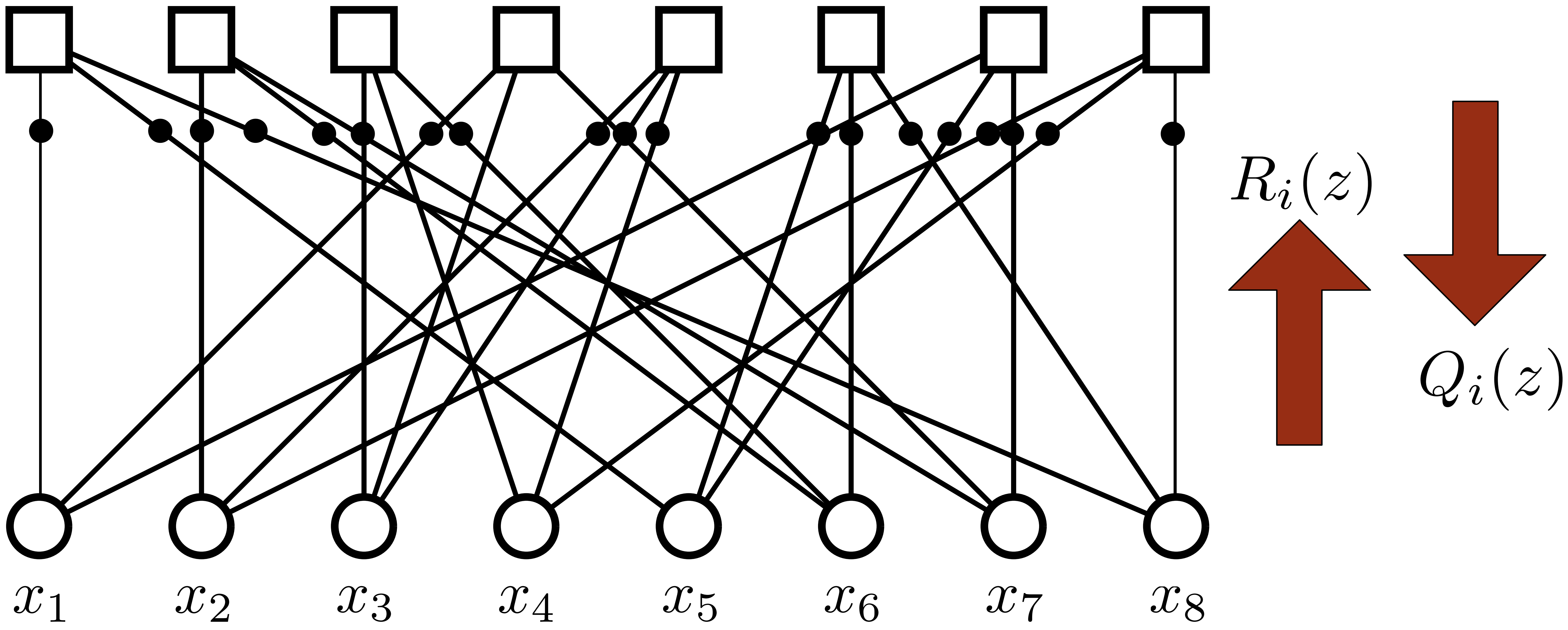
"parity check" integer $\mathbf{b}$

$$H\mathbf{x} = \mathbf{b}$$

Check node:

$x_1 + x_2 + x_3 = b$

(over real numbers)



Check Node: Convolution

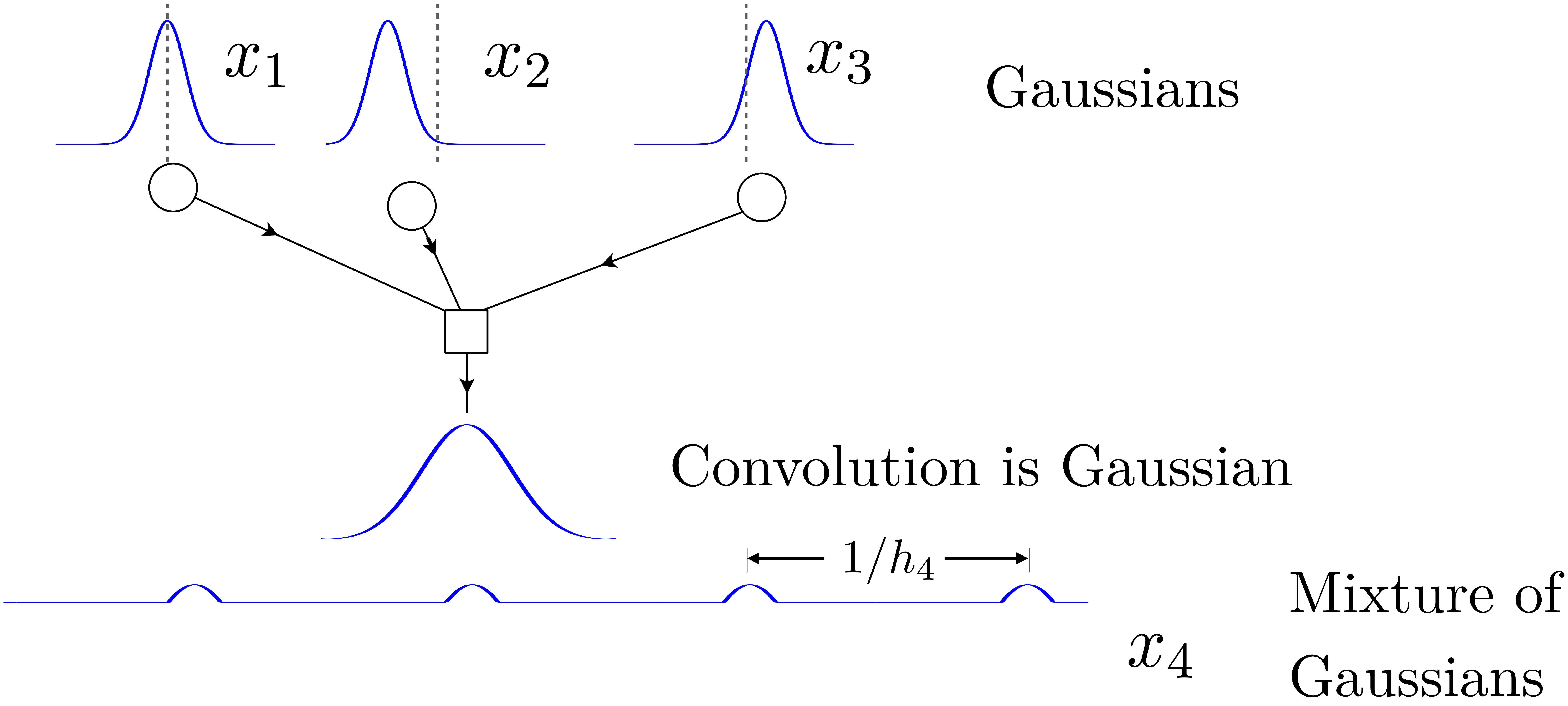
$$b_i \quad = \quad x_1 + \quad x_2 + \quad x_3 + \quad x_4$$

then consider <u>coefficients</u>...

Check Node: Convolution

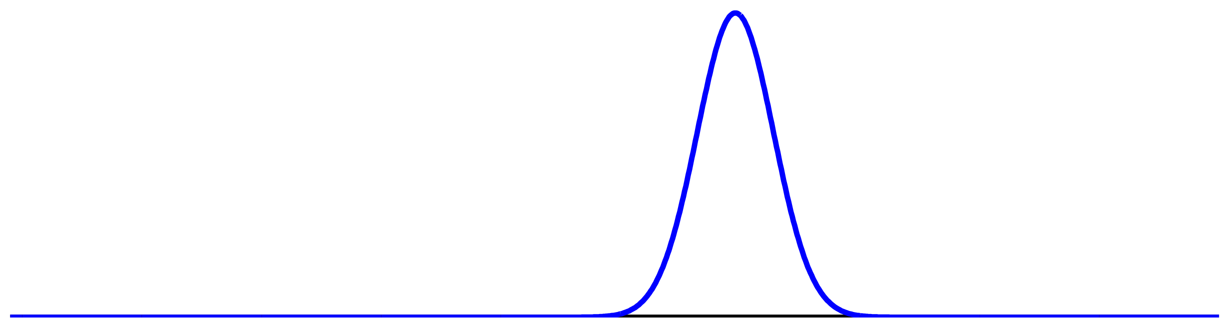
$$b_i \quad = \quad h_1 x_1 + h_2 x_2 + h_3 x_3 + h_4 x_4$$

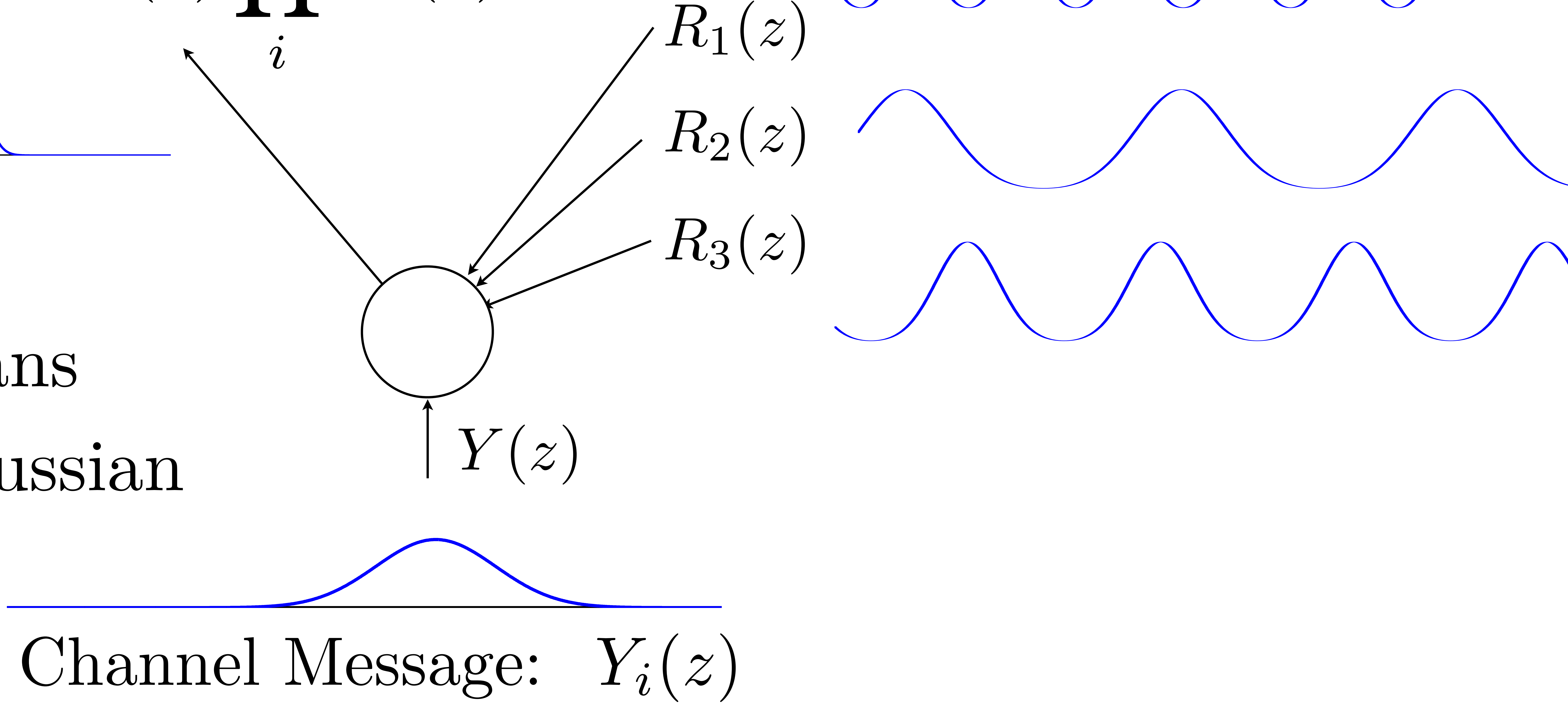
Check Node: Convolution



Variable Node: Combine Beliefs

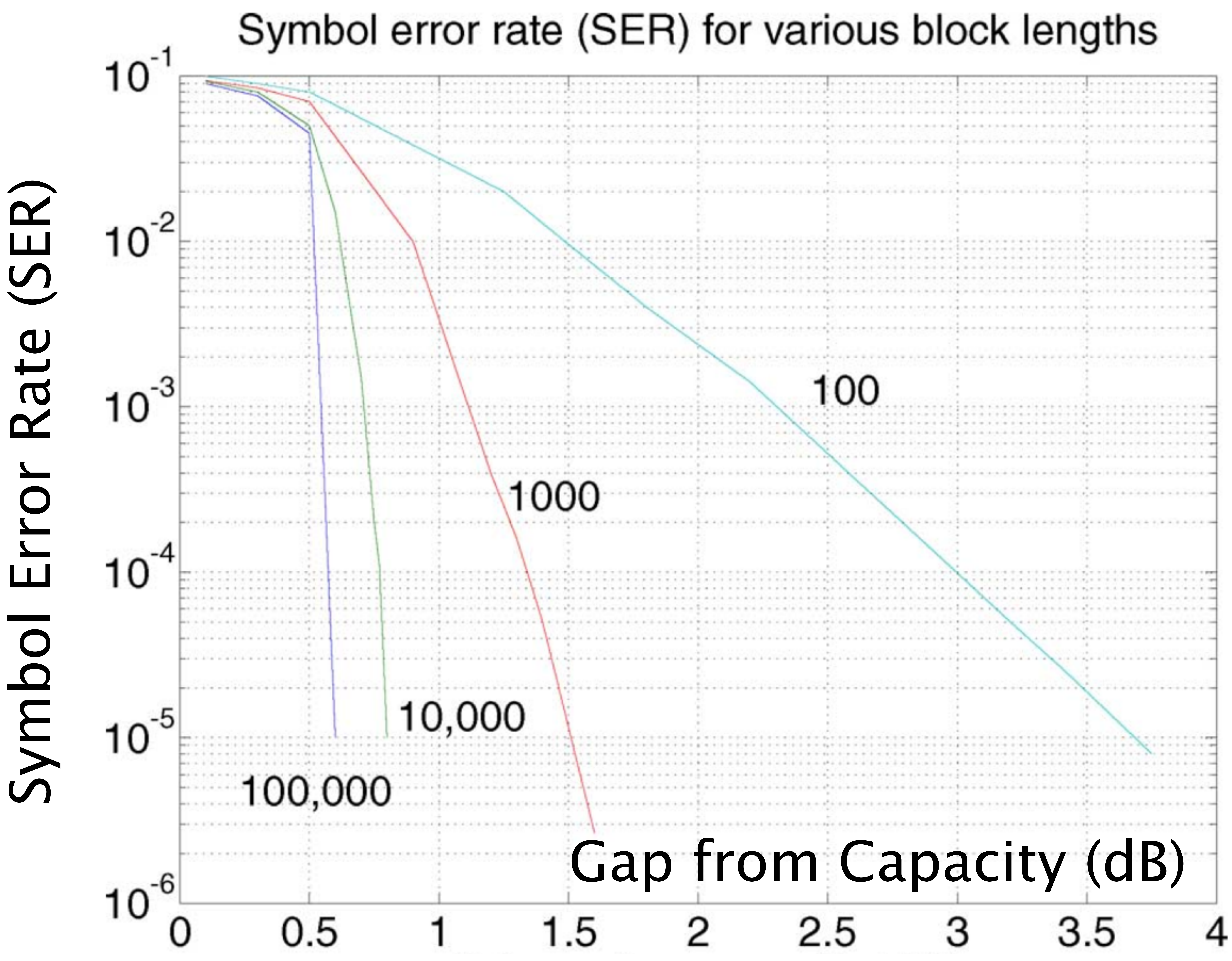
$$Q(z) \propto Y(z) \prod_i R_i(z)$$





Product of
mixture of Gaussians
is a mixture of Gaussian

LDLC Iterative Decoding



N. Sommer and M. Feder and O. Shalvi, "Low-Density Lattice Codes," IEEE Trans. Info. Theory, July 2008

(1d) Design of Latin Square LDLCs

Latin square: each row/column $\{h_1, h_2, \ldots, h_d\}$ $h_1 \geq h_2 \geq \ldots \geq h_d$

How to select d and h_i?

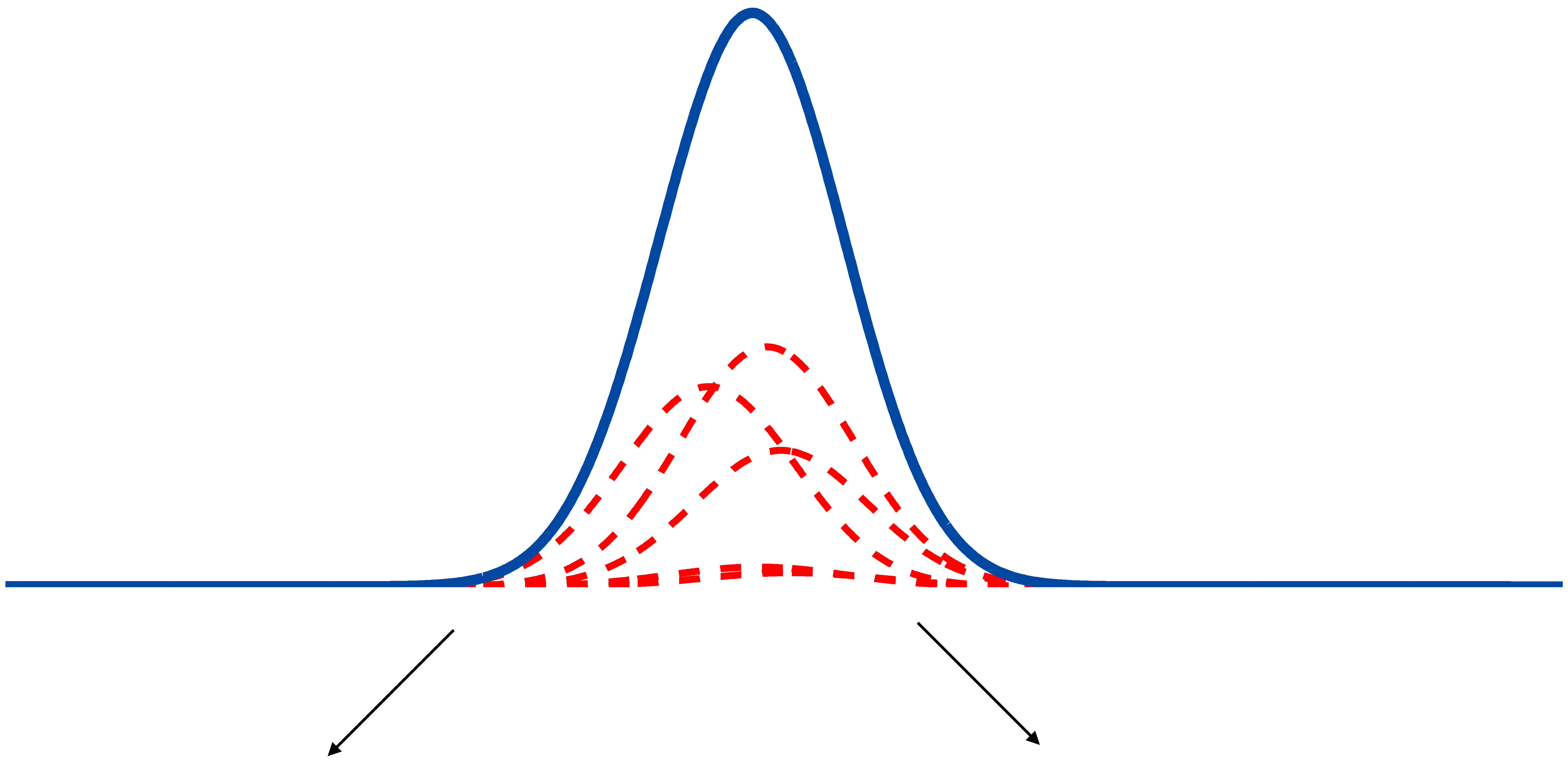
Choose $h_1 = 1$ to normalize the power

Convergence condition: $\frac{\sum_{i=2}^{d} h_i^2}{h_1^2} \leq 1$ (next section)

Empirical observations:

- Increasing degree d improves performance until $d = 7$
- Choice of h_2, h_3, ... not so important. Practical benefit for $h_2 = h_3 = \ldots$

Gaussian Mixtures



2. Condition on convergence of variances

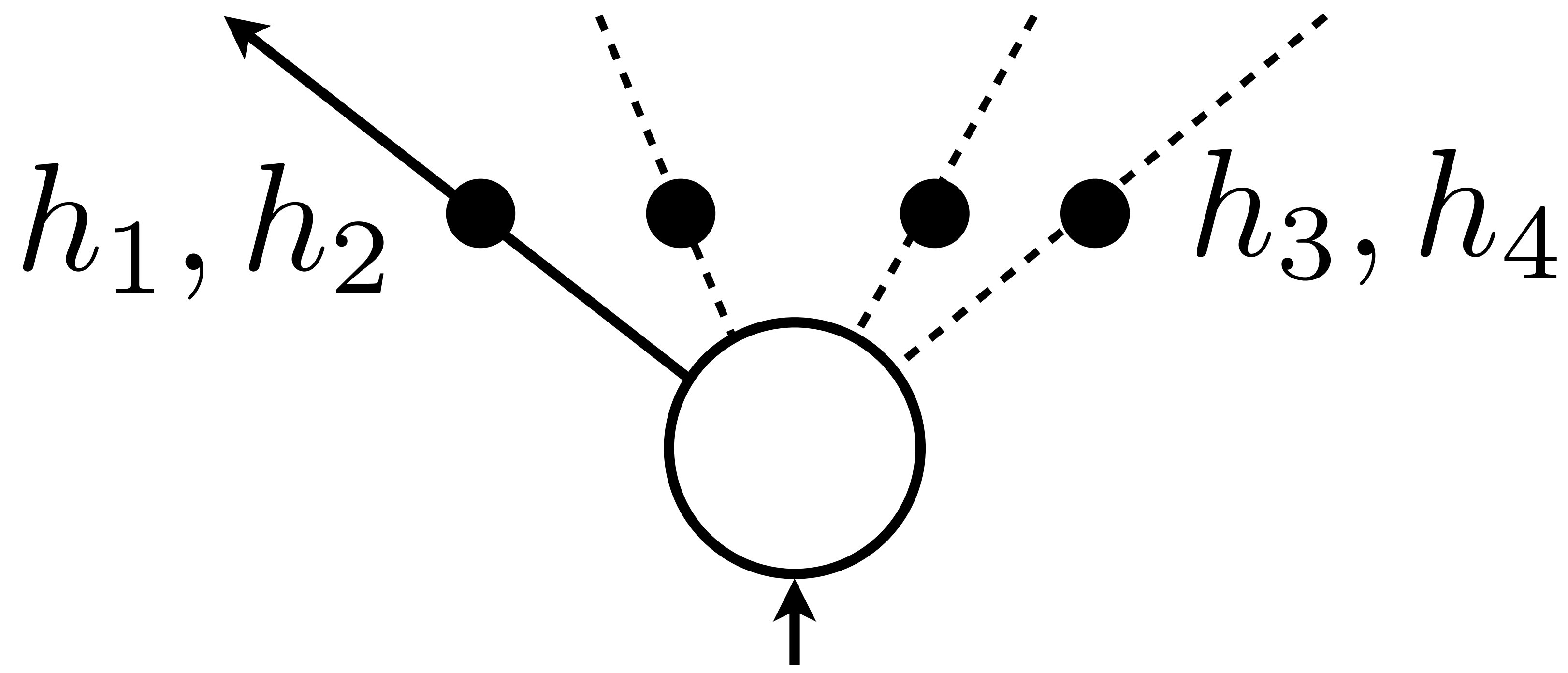
3. Gaussian BP Approximation of Gaussian mixture

(2) Convergence Condition on Variances

All mixture components have the same variance

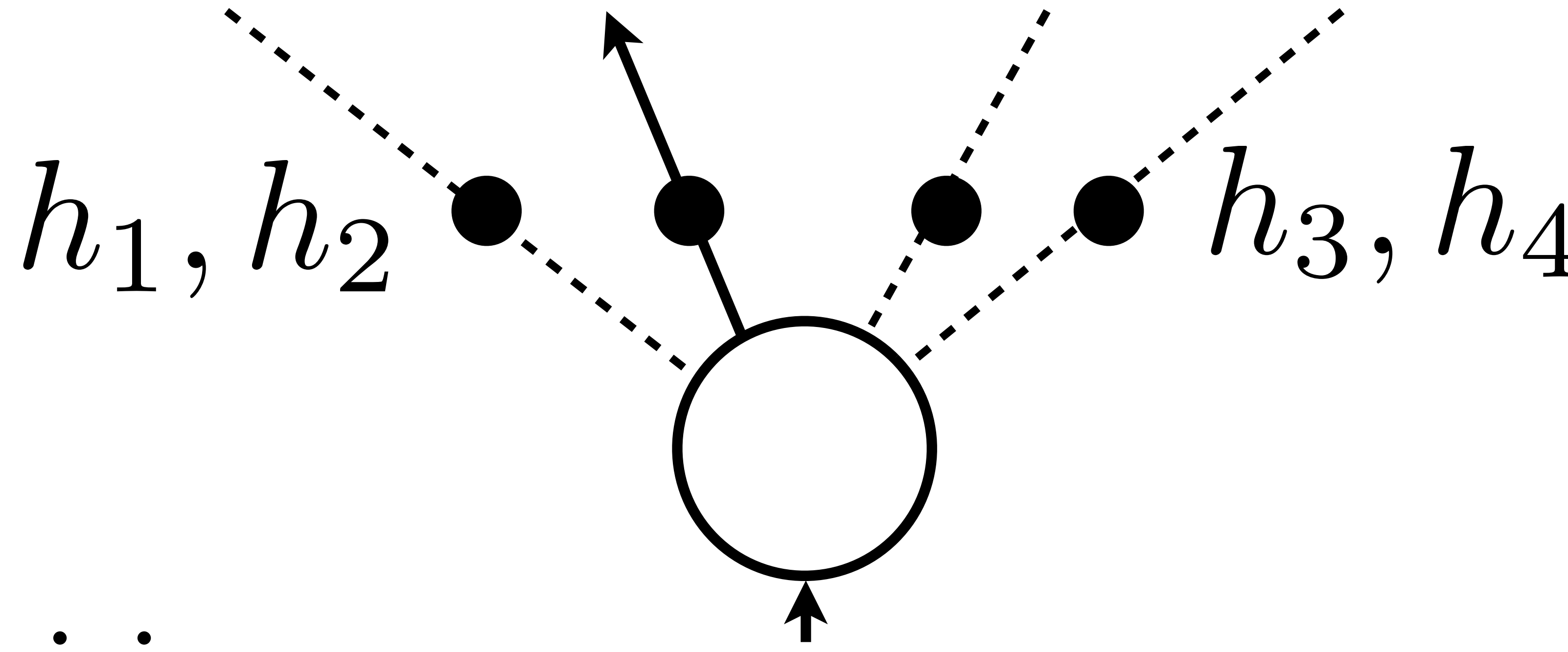
At variable node, two types of outgoing messages:

wide messages



- outgoing message on edge h_1 outgoing
- if alpha < 1, variance converges to a non-zero constant

narrow messages



- outgoing message on edge h_2, h_3,...
- if alpha < 1, variance converges to 0

  — sufficient for convergence of variance in final decisions

Convergence of the variances

$$v_i^{(0)} = \sigma^2$$
$$v^{(\ell+1)} \leq \alpha v^{(\ell)}$$
$$\Rightarrow v_i^{(\ell)} \leq \alpha^\ell \sigma^2$$

Theorem Define α as:

$$\alpha = \frac{\sum_{i=2}^{d} h_i^2}{h_1^2}.$$

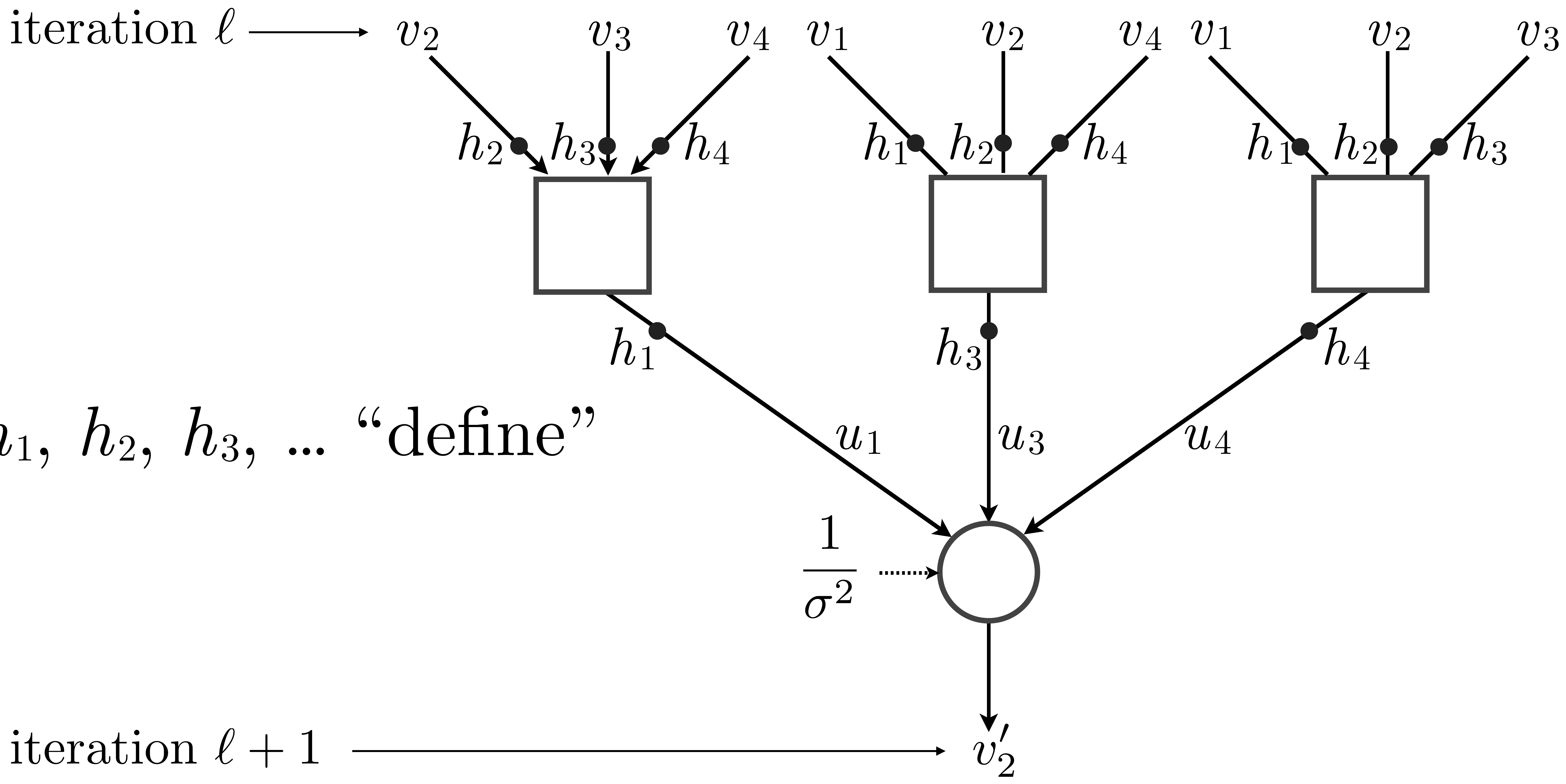
Then:

1. On iteration ℓ, the variances are upper bounded as:
$$v_i^{(\ell)} \leq \alpha^\ell \sigma^2$$
for $i = 2, \ldots, d$.

2. The asymptotic value of $v_1^{(\infty)} = \lim_{\ell \to \infty} v_1^{(\ell)}$, is:
$$v_1^{(\infty)} = (1 - \alpha)\sigma^2$$

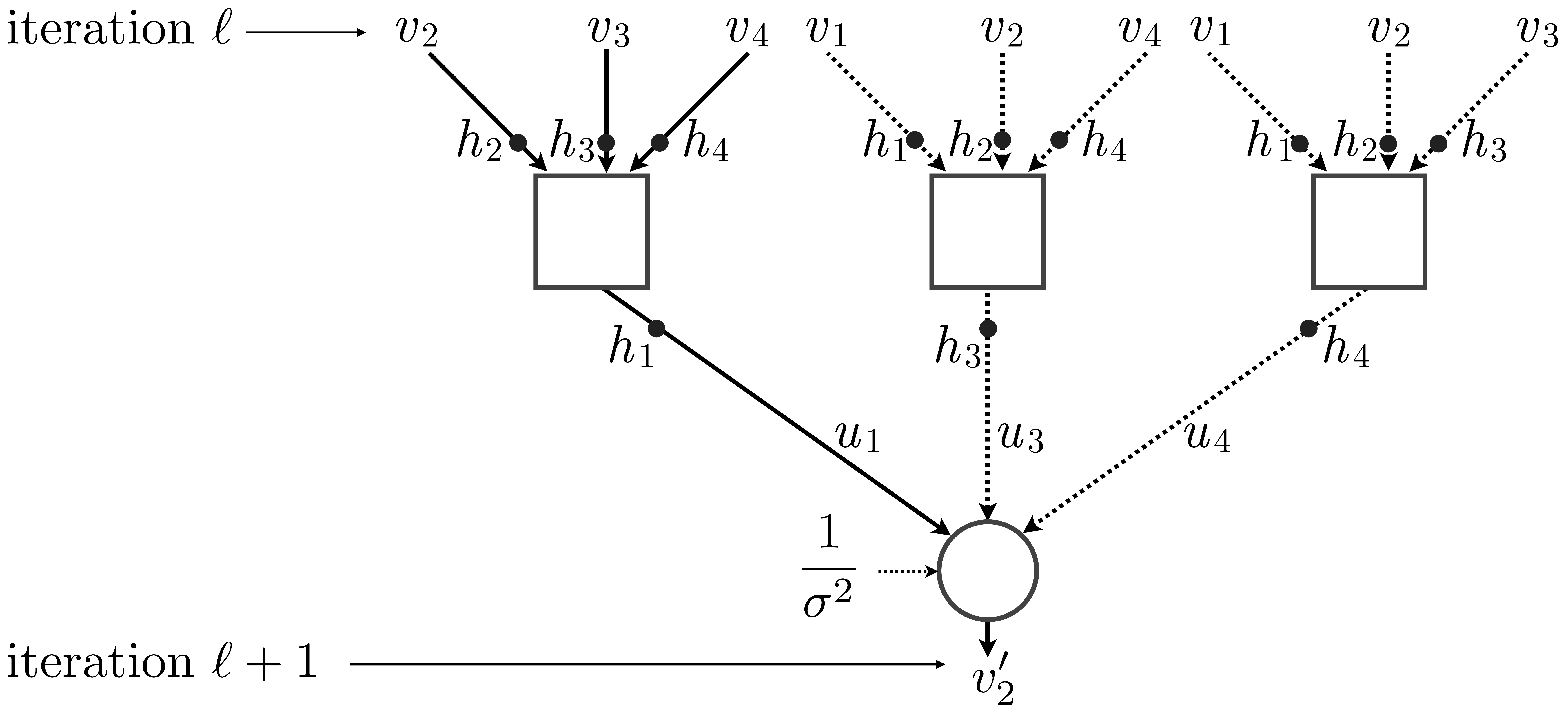
N. Sommer and M. Feder and O. Shalvi, “Low-Density Lattice Codes,” IEEE Trans. Info. Theory, July 2008

Recursion of “narrow” variances

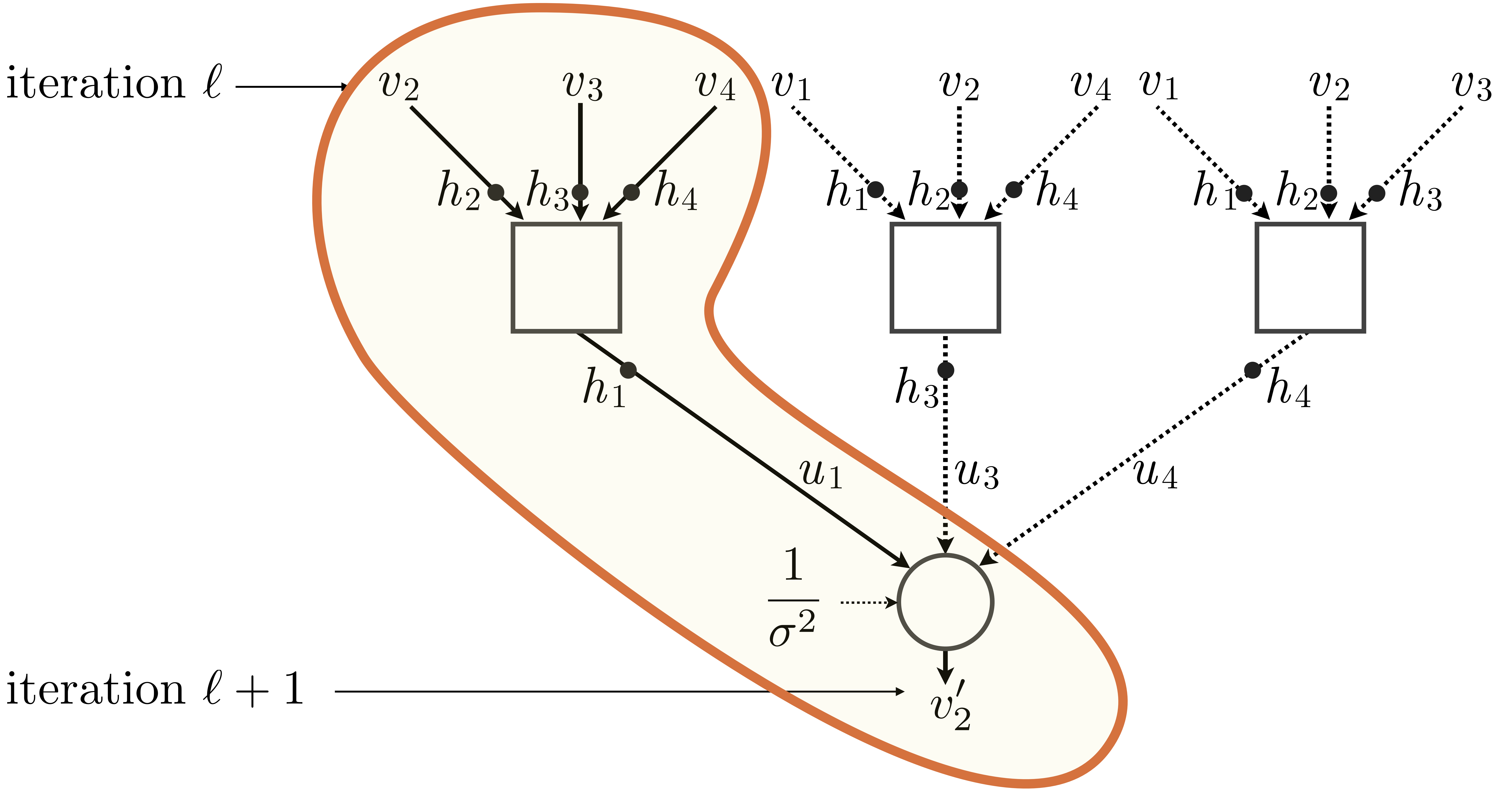


Which h_1, h_2, h_3, ... “define” alpha?

Recursion of “narrow” variances



Recursion of "narrow" variances



Generalization of Convergence to Non-Latin Square

- Multiply each row of H by c_i

$$\alpha = \frac{\sum_{i=2}^{d} c^2 h_i^2}{c^2 h_1^2} \rightarrow \frac{\sum_{i=2}^{d} h_i^2}{h_1^2} \leq 1$$

- Non-Latin square that satisfies a convergence condition
- Possibly changing $|\det H|$
- useful for triangular constructions where non-uniform coefficients are needed

(3) Decoding. Moment Matching: Replace Gaussian Mixture with A Single Gaussian Approx.

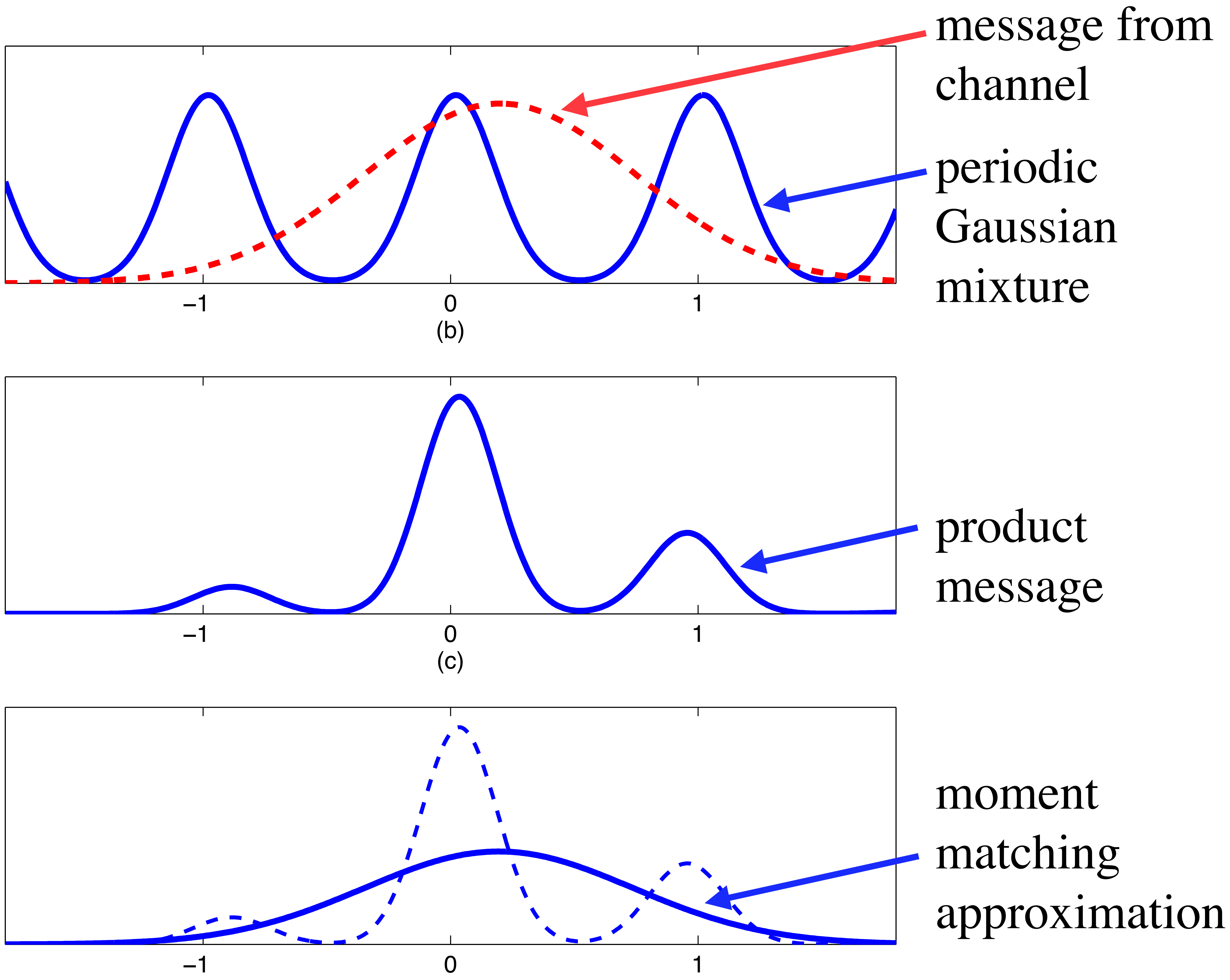
<u>Moment matching</u>

Single Gaussian has same mean and variance of the Gaussian mixture:

$$\begin{aligned} E[Y] &= c_1 m_1 + c_2 m_2 \\ E[Y^2] &= c_1 \cdot (v_1 + m_1^2) + c_2 \cdot (v_2 + m_2^2) \end{aligned}$$

Very efficient!

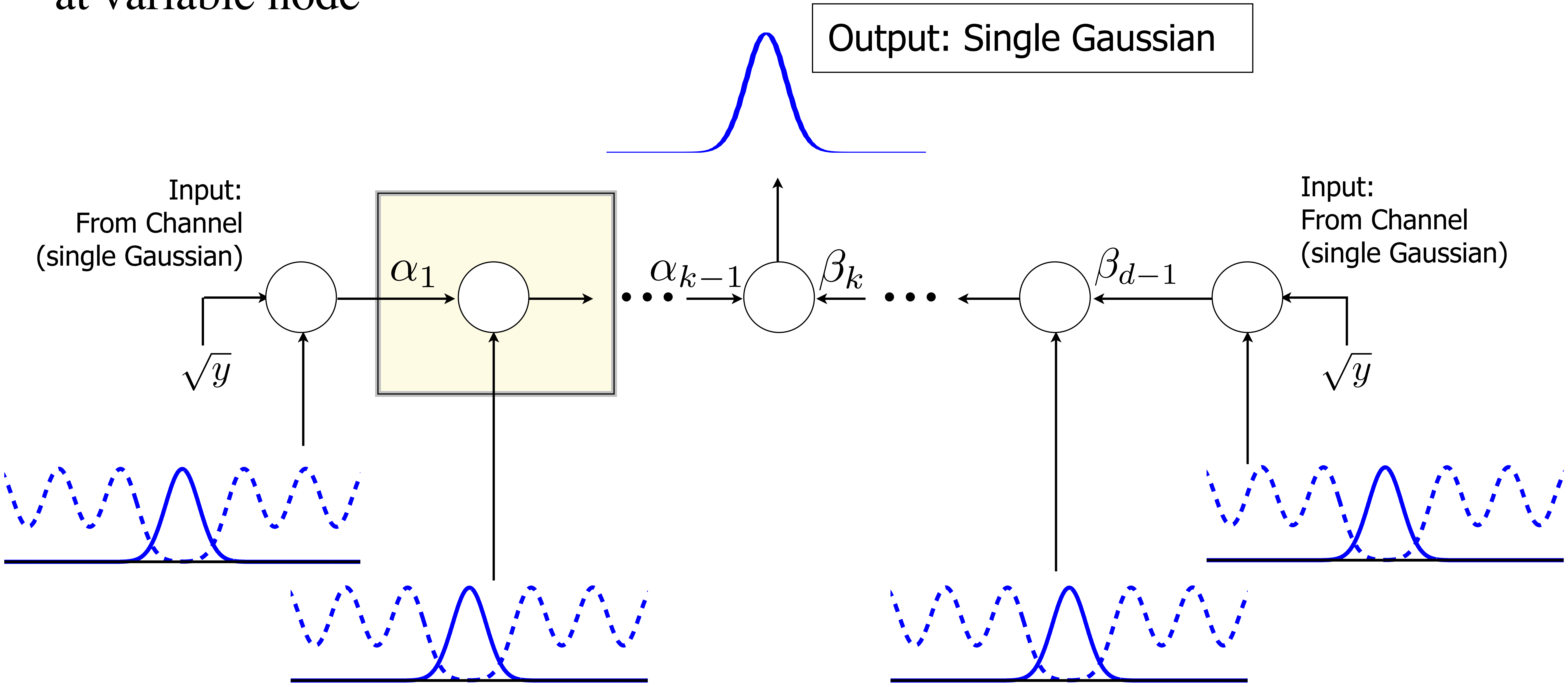
Moment matching results in minimizing the Kullback-Leiber divergence



Rasmussen and Williams, *Gaussian Processes for Machine Learning*. The MIT Press, 2005

Single Gaussian Decoder: Variable Node

Forward-backward algorithm
at variable node



Noise Thresholds under Single-Gaussian Approximation

Monte Carlo density evolution

0.1 dB gap to $n = 100{,}000$ lattice

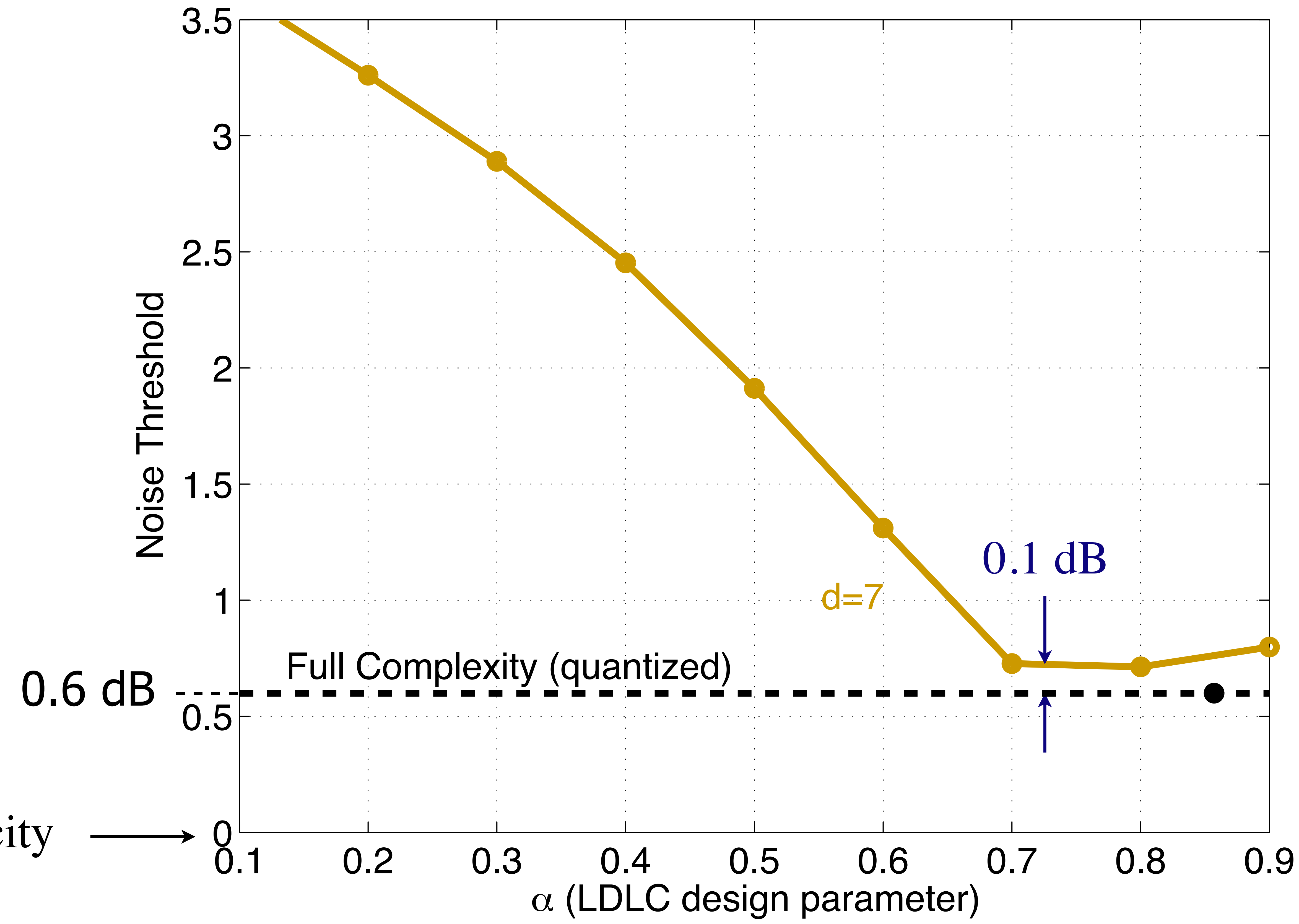
$\rightarrow$ small quantization loss

computationally simple

row/column weight $d = 7$

is good choice

$\alpha \approx 0.7$–0.8 is good choice



"Single-gaussian messages and noise thresholds for decoding low-density lattice codes," ISIT, 2009.

Single-Gaussian, Finite-Length LDLC

Gaussian Mixture Reduction Algorithm

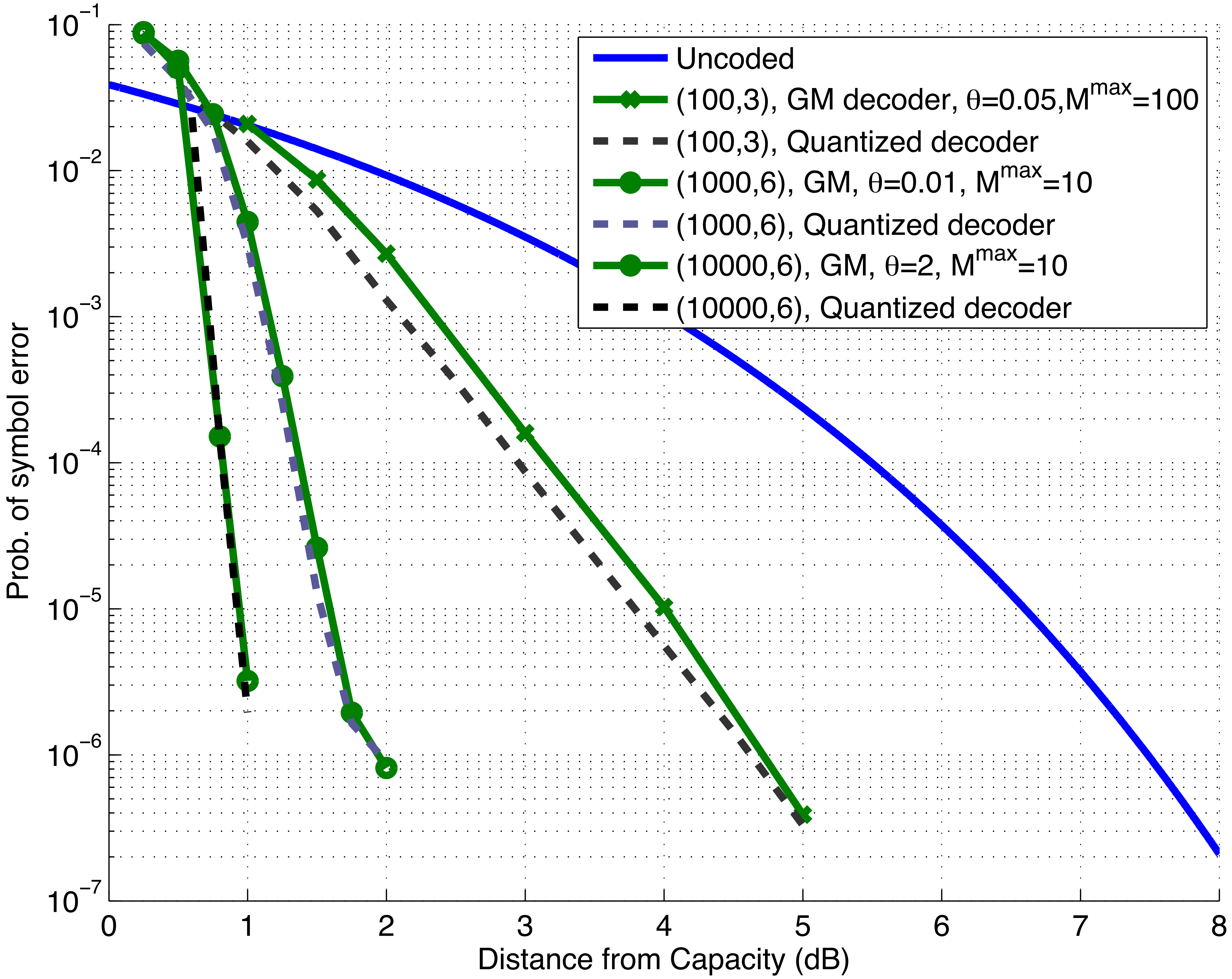
Gaussian mixture reduction algorithm allow 2 or more Gaussians in the approximation.

Messages between check/var are single Gaussian → low memory

Same performance as quantized messages

Algorithm is greedy combining with two parameters

Would like some improvements



"Reduced-memory decoding of low-density lattice codes," IEEE Communications Letters, vol. 14, pp. 659-661, July 2010.

Summary of Gaussian Decoders

	Density Evolution	Finite-dimension
Single Gaussians Everywhere	✅	❌
Gaussian mixtures internally at variable node Single Gaussians between var/check node	✅	✅

(4) LDLCs vs. Construction A & D

"Why not construct lattices from codes we already know?"

p-ary LDPC + Construction A = Lattice

- generally $p \to$ infinity to achieve capacity
- decoding p-ary LDPCs requires more storage than Gaussian BP
- "Not every lattice can be described by Construction A"

Problems with termination

- Construction D Spatially-Coupled LDPCs [Vem et al., ISIT 2014]

  0.106 from capacity (ignoring rate loss) 0.952 dB with rate loss
- Turbo codes + Construction D have termination problems [Sakzad et al]
- Triangular LDLCs have a slight rate loss [Sommer et al., ITW 2008]

Future Directions and Open Problems

Want practical lattices/decoder to achieve recent information-theoretic results

Low-density lattice codes, Gaussian BP decoding, few tenths of dB to capacity

Near future

- Gaussian BP decoder more elegant than "Mixture Reduction Algorithm"
- Beyond Latin square: improving the design of LDLC lattices
- Shaping for AWGN power constraint [Mo2C: Lattice Codes, 13:40 today]

Open problem

- Can LDLC lattices achieve capacity? Loeliger-like result for LDLCs